CLAIMS:

1. In an information handling system for identifying network resources comprising packets of data received from a network, a method comprising:

receiving a network resource comprising one or more packets, each packet comprising a header and data portion;

scanning the bytes of the one or more packets to determine the application-level protocol, and thus the application, the sender of the bytes is using.

parsing the bytes of the one or more packets according to the specific application-level protocol to extract identifying information relating to a specific resource requested;

comparing the extracted information to a list of identifying information stored in a real-time database; and

providing a message indicating that the extracted information matches at least one entry in the real-time database when the comparison is positive.

2. The method of claim 1, wherein the receiving step comprises receiving a plurality of packets according to the Transmission Control Protocol.

3. The method of claim 1, wherein the receiving step comprises receiving a plurality of packets according to the User Datagram Protocol.

4. The method of claim 1 wherein the one or more packets use the hypertext transfer protocol, the scanning step comprises extracting a destination domain name or IP address from a hypertext transfer protocol packet stream and the comparing step comprises comparing the address extracted with addresses stored in the database.

5. The method of claim 1 wherein the one or more packets follow the hypertext transfer protocol and the scanning step further comprises extracting the port, path, and name of the web resource from a hypertext transfer protocol packet stream.

6. The method of claim 1 wherein, the scanning step comprises extracting a hash code from a received peer to peer protocol packet stream.

7. The method of claim 1 wherein, the scanning step comprises extracting additional information comprising port, identity key, and filename from a peer to peer protocol packet stream.

8. The method of claim 1 wherein, the scanning step comprises extracting a user agent name, additional HTTP extension headers, or other information needed to identify a specific program from a peer to peer protocol packet stream.

9. The method of claim 1 wherein, the scanning step comprises extracting a filename and path received from a file transfer protocol packet stream.

10. The method of claim 1 wherein the scanning step further comprises detecting a transmission control protocol connection to an external simple mail transfer protocol server, and limiting access to the external simple mail transfer protocol server.

11. The method of claim 1 further comprising logging all instant message communication.

12. The method of claim 1 further comprising providing a message announcing a match upon identifying the match.

13. The method of claim 1 wherein, the comparing step, upon identifying a match, further comprises blocking the user from accessing the resource corresponding to the matching identifying information.

14. The method of claim 1 wherein the identifying information corresponds to illegal copies of files.

15. The method of claim 1 wherein the identifying information corresponds to prohibited resources.

16. The method of claim 1 wherein the scanning step comprises extracting an IP address from at least one packet and the comparing step comprises comparing the IP address with a set of IP addresses stored in the database.

17. The method of claim 1 wherein the identifying information comprises a hash code.

18. The method of claim 1 wherein the identifying information corresponds to suspicious files and wherein a client requesting a file whose identifying information matches an identifying information stored in the database is presented a warning.

19. The method of claim 1 wherein, the comparing step upon identifying a match further comprises limiting access by clients to external simple mail transfer protocol servers.

20. The method of claim 1 further comprising using identifying information found by a central server farm comprising specialized search engines and a human staff to populate the database.

20. The method of claim 13 wherein the blocking step is accomplished by ending client/server communication for a request that contains the matching identifying information.

21. The method of claim 13 wherein the blocking step is accomplished by ending client/server communication for a response that contains the matching identifying information.

22. The method of claim 1 wherein the receiving step comprises receiving a plurality of packets according to the Simple Mail Transfer Protocol.

23. The method of claim 1, wherein the scanning step further evaluates additional headers and the data portion of the hypertext transfer protocol, such as web forms on an html page, based on the address.

24. A system comprising:

a network interface for receiving data packets from a network;

a processor for extracting identifying information from the data packets and for comparing the extracted identifying information with the identified information stored in a database; and

an output for providing a message stating when a match has been found.

25. The system of claim 24 further comprising a memory for storing the identified information to be compared with the information extracted from the received packets.

26. A local area network comprising a network gateway device comprising: a network interface for receiving data packets; a processor for extracting identifying information and for comparing the extracted identifying information with the identifying information stored in a database; and an output for providing a message stating that a match has been found when the comparison is positive.

27. The local area network of claim 26 further comprising the database.

28. The local area network of claim 26 further comprising a router disposed between the network gateway device and a firewall connecting the local area network to a wide area network.

29. The local area network of claim 26 further comprising a load balancer disposed between the router and a firewall.

30. The local area network of claim 26 further comprising a network gateway device disposed between a router and a load balancer.

31. The local area network of claim 26 further comprising a load balancer disposed

between the network gateway device and a firewall connecting the local area network to a wide area network.

32. The local area network of claim 26 further comprising a router containing the network gateway device.

33. The local area network of claim 26 further comprising a firewall disposed between the router containing the network gateway device and the wide area network.

34. The local area network of claim 26 further comprising a firewall containing the network gateway device.

35. The local area network of claim 26 further comprising the firewall containing the network gateway device disposed between a router and the wide area network.